Shubham Patel - 201901100

Page No. : 1

Date :

SC402 HW-2

[1] $x \in \{2, 3, 4, 5, \ldots, 12\}$ and $y \in \{D, N\}$

x	y	$P_x[x, y]$	$P_x[x \mid y]$	$P_x[y \mid x]$
2	D	1/36	1/6	1
3	D	-	-	-
4	D	1/36	1/6	1/3
5	D	-	-	-
6	D	1/36	1/6	1/5
7	D	-	-	-
8	D	1/36	1/6	1/5
9	D	-	-	-
10	D	1/36	1/6	1/3
11	D	-	-	-
12	D	1/36	1/6	1
2	N	0	0	0
3	N	2/36	2/30	1
4	N	2/36	2/30	2/3
5	N	4/36	4/30	1
6	N	4/36	4/30	4/5
7	N	6/36	6/30	1
8	N	4/36	4/30	4/5
9	N	4/36	4/30	1
10	N	2/36	2/30	2/3
11	N	2/36	2/30	1
12	N	0	0	0

there are total $n = 36$ possibilities.

[2] given, $Pr[K_1] = Pr[K_2] = Pr[K_3] = \alpha/3$

$Pr[K_4] = Pr[K_5] = \beta/2$

$Pr[a] = 1/3 \quad Pr[b] = 2/3$

(1)

$Pr[c=1] = Pr[K_1] \cdot Pr[a] + Pr[K_3] \cdot Pr[b]$

$= \alpha/3$

$Pr[c=2] = \alpha/3$

$Pr[c=3] = \alpha/3$

$Pr[c=4] = Pr[c=5] = \beta/2$

Now,

$$Pr[p=a \mid c=1] = \frac{Pr[a] \cdot Pr[c=1 \mid p=a]}{Pr[c=1]}$$

$$= \frac{Pr[a] \cdot Pr[k=k_1]}{Pr[c=1]}$$

$$= \frac{1/3 \cdot \alpha/3}{\alpha/3}$$

$$= \frac{1}{3} = Pr[p=a]$$

- now, same for other possibilities

$Pr[p=b \mid c=1] = 2/3 = Pr[b]$

$Pr[p=a \mid c=2] = 1/3 = P[a]$

$Pr[p=b \mid c=2] = 2/3 = P[b]$

$Pr[p=a \mid c=3] = Pr[p=a \mid c=4] = Pr[p=a \mid c=5]$

$= 1/3 = P[a]$

$Pr[p=b|c=3] = Pr[p=b|c=4] = Pr[p=b|c=5]$
$= 2/3 = Pr[b]$

- So for $\forall x \in p$ and $y \in c$
- $Pr[x|y] = Pr[x]$
- So this crypto system achieves perfect secrecy.

[3] $\forall x, y \in Z_{26}$ and $\forall a \in Z_{26}^*$, there exist unique $b(x, y, a) \in Z_{26}$ such that $e(a, b(x, y, a))(x) = y$

$$Pr[y=y] = \sum_{x \in \{1,\dots n\}} \sum_{a \in Z_{26}^*} Pr[k=(a, b(x,y,a))] Pr[x=x]$$
$$= 1/26$$

- For any $x, y \in Z_{26}$
$$Pr[Y=y|X=x] = \sum_{a \in Z_{26}^*} Pr[k=(a, b(a,b,x))]$$
$$= 1/26$$
- Using Baye's theorem,
$Pr[X=x|Y=y] = Pr[X=x]$
- So if we use every key with equal probability. $1/312$ then we can get perfect secrecy.

(b) For any $y \in \{1, 2, \ldots, n\}$

- $Pr[Y = y] = \sum_{x \in \{1,2,\ldots n\}} \sum_{a \in Z_{26}^*} Pr[k = (a, b(x, y, a))] Pr[x]$
  $= 1/26$

- For any $x, y \in Z_{26}$
  $Pr[Y = y \mid X = x] = \sum_{a \in Z_{26}^*} Pr[k = (a, b(x, y, a))]$
  $= 1/26$

- Using Bayes theorem,
  $Pr[X = x \mid Y = y] = Pr[X = x]$

[4] Lets say, 'S' takes value from $\{2, 3, \ldots, 12\}$ = sum of pair of dice

- $n = 36$
- $Pr[S = 2] = 1/36$
  $Pr[S = 3] = 2/36$
  $Pr[S = 4] = 3/36$
  $Pr[S = 5] = 4/36$
  $Pr[S = 6] = 5/36$
  $Pr[S = 7] = 6/36$
  $Pr[S = 8] = 5/36$
  $Pr[S = 9] = 4/36$

$P_r[S=10] = 3/36$

$P_r[S=11] = 2/36$

$P_r[S=12] = 1/36$

- Now,

$$H(S) = \frac{\log_2 36}{36} \cdot 2 + \frac{\log_2 36 - 1}{36} \cdot 4 + \frac{\log_2 36 - \log_2 3.6}{36} + \frac{\log_2 36 - 2}{36} \cdot 8 + \frac{\log_2 36 - \log_2 3.10}{36} + \frac{\log_2 36 - \log_2 6}{36} \cdot 6$$

$H(S) = 2.94$

[5] $P = \{a, b, c\}$

$P_r[a] = 1/2 \quad P_r[b] = 1/3 \quad P_r[c] = 1/6$

$k = \{k_1, k_2, k_3\}$

$P_r[k_1] = P_r[k_2] = P_r[k_3] = 1/3$

$c = \{1, 2, 3, 4\}$

- $H[P] = \frac{\log_2 2}{2} + \frac{\log_2 3}{3} + \frac{\log_2 6}{6}$

$= 1.46$

$$H(K) = \frac{\log_2 3}{3} + \frac{\log_2 3}{3} + \frac{\log_2 3}{3}$$

$$= 1.58$$

- NOCO,

$$P_r[C=1] = P_r[a] \cdot P_r[K_1] + P_r[c] \cdot P_r[K_3]$$

$$= 2/9$$

$\therefore P_r[C=2] = 5/18$

$P_r[C=3] = 1/3$

$P_r[C=4] = 1/6$

$$H(C) = \frac{2}{9}(\log_2 9 - \log_2 2) + \frac{5}{8}(\log_2 18 - \log_2 3) + \frac{1}{3}(\log_2 3) + \frac{1}{6}(\log_2 6)$$

$$= 1.95$$

$$H(K|C) = H(K) + H(P) - H(C) = 1.09$$

- For H(P|C),

$P_r[P=a, y]$ $y = 1, 2, 3$

$= 1/6$

$P_r[P=b, y] = 1/9$ $\quad y = 2, 3, 4$

$P_r[P=c, y] = 1/18$ $\quad y = 1, 3, 4$

$$H(P,C) = 3\left(\frac{\log_2 6}{6} + \frac{\log_2 9}{9} + \frac{\log_2 18}{18}\right)$$

$$= 3.044$$

$$H(P|C) = H(P,C) - H(C)$$

$$= 1.094$$